Journal of Computer and Communications, 2014, 2, 25-30
Published Online March 2014 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2014.24004

Scientific Research

Biometric-PKI Authentication System Using Fingerprint Minutiae

Han-Ul Jang, Heung-Kyu Lee*

Department of Computer Science, Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea
Email: *hklee@mmc.kaist.ac.kr

Received October 2013

Abstract

A digital certificate under Public Key Infrastructure has a defect of Man-in-the-Middle Attack that performs hash collision attacks. In this paper, we propose a robust biometric-PKI authentication system against Man-in-the-Middle Attack. The biometric-PKI authentication system consists of current PKI authentication and biometric authentication, which employs biometric data and a public key from a digital certificate. In the proposed biometric-PKI authentication system, an authentication process performs that it extracts consistent features of fingerprint images, encrypts consistent features, and matches features with prepared templates. The simulation results of the proposed authentication system prove that our system achieves low false acceptance rate and high accuracy rate.

Keywords

Biometrics; PKI Authentication; Fingerprint Minutiae

1. Introduction

Public Key Infrastructure (PKI) [1,2] is a foundation technology for handling key distribution and validation in communication security. PKI has widely employed for highly secured key management since 1990's.

PKI enables secure key distribution that is the main issue in communication security. For instance, it is the most secure method that user A delivers own secret key to user B in person, however, the method has very low scalability. PKI has an automated process for secure key distribution.

Although PKI has an important benefit in communication security, the more phishing and Man-in-the-Middle Attack (MITM Attack) have emerged, the often the security of PKI has been weakened. Currently, it is a common opinion that PKI contains drawbacks on a variety of communication attacks. Hence, PKI could not be comprehensive security solution any longer.

Under PKI, it is difficult to trust a public key of a digital certificate with the only key information. For instance, a tampered public key could be trusted if an attacker uses MD5 hash collision attack to the public key since the tampered public key could be validated by a digital certificate of Certificate Authority (CA). Providing a comprehensive security solution with only PKI causes very dangerous situation in communication security.

*Corresponding author.

How to cite this paper: Jang, H.-U. and Lee, H.-K. (2014) Biometric-PKI Authentication System Using Fingerprint Minutiae. *Journal of Computer and Communications*, **2**, 25-30. http://dx.doi.org/10.4236/jcc.2014.24004

Biometrics describes recognition technologies on unique physiognomy or behavior properties that human beings have. Biometric data provides enhanced non-repudiation beside PKI due to their unique information. Biometric data could be a component of user authentication, moreover it improves degree of security in communication integrating other authentication systems. However, biometric information has a fatal defect that it must not be used if the biometric data is leaked. Hence, it is significantly important to create cancelable biometric data that is irreversible.

Previous works on integration of biometrics and PKI that are robust to MITM Attack have introduced recently. Althobaiti *et al.* proposed an enhanced cryptography for biometric [3]. The proposed method creates public key-pair employing elliptic curve, which is a NP-Hard problem, and biometric data. The cryptographic method has a benefit having higher security than that of PKI, whereas, the method requires the same features of biometric data to make the same secret key every time. Scheirer *et al.* presented an anti-MIM Attack scheme creating revocable biotokens [4]. However, the scheme could be done under an exceedingly ideal case, so it has limitation of generating a practical revocable biotoken.

In the following sections we will describe in detail our biometric-PKI authentication system. Sections 2 and 3 describe the algorithm on detection of fingerprint core point and the method on detection of minutiae of fingerprints, respectively. In Section 4, MITM Attack is described using a scenario. Section 5 mainly discusses our biometric-PKI authentication algorithm. Section 6 and Section 7 contain the experimental results and the summary, respectively.

2. Fingerprint Core Point Detection

In order to obtain consistent features from fingerprint images, fingerprint core point detection is essential. To find a core point of a fingerprint, which the core point is illustrated in **Figure 1**, a fingerprint image is enhanced under two preprocessing steps including normalization and orientation field detection [5,6]. Finally, core point detection performs with an orientation field of a fingerprint.

2.1. Normalization

Let $I(i, j)$ and $N(i, j)$ denote the original pixel (i, j) and the normalized gray-level value (i, j), respectively. The normalization of a fingerprint image is defined as

$$N(i,j)=\begin{cases} M_0+\sqrt{\dfrac{V_0\left(I(i,j)-M_i\right)^2}{V_i}} & \text{if } I(i,j)>M \\ M_0-\sqrt{\dfrac{V_0\left(I(i,j)-M_i\right)^2}{V_i}} & \text{otherwise} \end{cases} \tag{1}$$

where M_i and V_i, the estimated mean and variant of $I(i, j)$, respectively. M_0 and V_0 are the desired mean and variant, respectively. Normalization reduces sensor noise of a fingerprint image and removes gray- level deformation caused by finger pressure difference.

2.2. Orientation Field Detection

An orientation field of a fingerprint can be calculated by estimating the local orientation of each local block that is divided by a non-overlapping block of size $W \times W$. To estimate an orientation field, Rao's algorithm is employed [7]. Rao's algorithm contains the following steps.

1) Divide a fingerprint image into a non-overlapping block of size $W \times W$;

2) Calculate gradients G_x and G_y of each block;

3) Estimate the local orientation of each block. The formula for estimating the local orientation is defined as follows:

$$\theta_o=\frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{W}\sum_{j=1}^{W}2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{W}\sum_{j=1}^{W}\left(G_x^2(i,j)-G_y^2(i,j)\right)}\right) \tag{2}$$

(a) (b)

Figure 1. An orientation field and ridge ending points of a fingerprint image. The core point is marked with a red circle; (a) is an orientation field image and (b) is an end-point image.

where W is the size of block, G_x and G_y are gradient magnitudes in x and y, respectively.

2.3. Core Point Detection

A core point of a fingerprint is detected by curvature technique. The algorithm is described as follows.

1) Compute the local orientation $\theta(i, j)$ using Equation (2) above;

2) Calculate the difference of orientation about each local block. The formula as follows:

$$Diff\ \mathrm{X} = \sum_{k=1}^{W} \cos 2\theta(W, k) - \sum_{k=1}^{W} \cos 2\theta(1, k) \tag{3}$$

and

$$Diff\ \mathrm{Y} = \sum_{l=1}^{W} \sin 2\theta(l, W) - \sum_{l=1}^{W} \sin 2\theta(l, 1) \tag{4}$$

where $Diff$ X and $Diff$ Y are the difference of orientation of columns and rows of a fingerprint image, respectively.

3) The curvature point X is located where both $Diff$ X and $Diff$ Y are negative.

4) If a core point of a fingerprint is not found, repeat core point detection until the core point is detected.

3. Minutiae Detection

Minutiae Detection is necessary process to create consistent features. The minutiae detection algorithm consists of the following steps [8,9].

1) A thinned ridge image R has eight neighbors such as $N_0, N_1, N_2, \ldots, N_7$ each pixel (x, y).

2) If pixel (x, y) has one neighbor as Equation (5), the pixel is a ridge ending point.

3) If pixel (x, y) has more than two neighbors as Equation (6), the pixel is a ridge bifurcation point.

4. MITM Attack

MITM Attack is an attack targeting at deficiency of the PKI authentication system. An attacker creates a pseudo-random public key applying hash collision attack to a certain user's digital certificate. The pseudo-random public key could be valid since the digital certificate including the tampered public key has the same hash value as the value of the original certificate. The attacker could read the data that is transmitted from the user when the MITM Attack succeeds. An attempt to attack a digital certificate under PKI presented at the 2008 Chaos Communications Congress [10]. The MITM Attack scenario is as follows.

1) An attacker creates a pseudo-random certificate that has the same hash value as the certificate of a certain user and establishes a rogue CA.

2) The user receives the tampered certificate and requests the rogue CA's certificate to validate the tampered

one.

3) The rogue CA transmits its own certificate to the user.

4) The user validates the tampered certificate using the rogue CA's certificate.

5) The user employs the tampered public key since the hash value is identical.

6) The attacker reads packets that are transmitted from the user with his/her own private key.

5. Biometric-PKI Authentication System

We propose a biometric-PKI authentication system and the whole process is shown in **Figure 2**. The proposed algorithm is as follows.

1) Find ridge ending points of a fingerprint image. Each ridge ending point has the distance of 10 from other points. If the distance is less than 10, the ridge ending point is excluded.

2) Calculate the distance between each ridge ending point and the core point. The distance is defined as Equation (7):

$$d_i = \left| X_0(x,y) - X_i(x,y) \right| \tag{7}$$

where X_0 and X_i are the core point and the i_{th} ridge ending point, respectively; d_i is the distance between X_0 and X_i.

3) Compute the difference of orientation between each ridge ending point and the core point. The difference of orientation is defined as Equation (8):

$$\Delta\theta_i = \left| \theta_0 - \theta_i \right| \tag{8}$$

where θ_0 and θ_i are the orientation of the core point and the i_{th} ridge ending point, respectively; $\Delta\theta_i$ is the difference of orientation between θ_0 and θ_i.

4) Quantize the distance and the difference of orientation. The quantization of distance and difference of orientation are defined as Equation (9) and (10), respectively:

$$d_i^Q = ceil(d_i / q_d) \tag{9}$$

$$\Delta\theta_i^Q = ceil(\Delta\theta_i / (\pi / q_\theta)) \tag{10}$$

where q_d and q_θ are quantization factors of distance and difference of orientation, respectively; d_i^Q and $\Delta\theta_i^Q$ are the i_{th} quantized distance and difference of orientation, respectively.

5) Obtain consistent features using quantized distance and difference of orientation. Consistent features are computed as

$$S_i = \mathrm{mod}((\rho\,\Delta\theta_i^Q + d_i^Q), \eta) \tag{11}$$

where S_i is the i_{th} consistent feature, ρ and η, a prime number which is used for differentiating each consistent feature and nonce, respectively. ρ could be less than 2^8 that is the sufficiently large number to use in Equation (11).

6) Divide a public key of a digital certificate into k coefficients. For instance, if the size of a public key is 1024-bit and k is 128, each coefficient has 8-bit, which each coefficient value is from 0 to 255.

$$C = \{C_1, C_1, C_1, \cdots, C_k\} \tag{12}$$

7) Encrypt consistent features as Equation (13):

$$E_i = \mathrm{mod}((C_1 \cdot \mathrm{mod}(S_i, M)^{k-1} + C_2 \cdot \mathrm{mod}(S_i, M)^{k-2} + \cdots + C_{k-1} \cdot \mathrm{mod}(S_i, M)^1 + C_k), M) \tag{13}$$

where E_i is the i_{th} encrypted consistent feature and M is a modulo operator that makes a number being

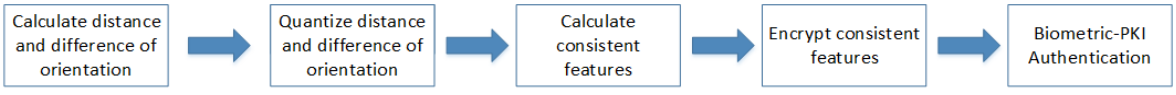


Figure 2. A flowchart of the proposed biometric-PKI authentication system.

calculated not exceed the limitation of an integer number. This step makes cancelable biometric features using the modulo operator M.

8) The proposed biometric-PKI authentication processes are as follows.

a) User A requests an access to Server S.

b) S transmits a nonce to A.

c) A sends his/her own digital certificate and encrypted consistent features E_A^{α} applying the nonce.

d) S validates A's certificate.

e) If A's certificate is valid, S creates encrypted consistent features E_A^{β} using A's fingerprint template and attempts biometric authentication.

f) If E_A^{α} and E_A^{β} have the maximum matching, the biometric authentication succeeds and S trusts A's public key.

6. Experimental Results

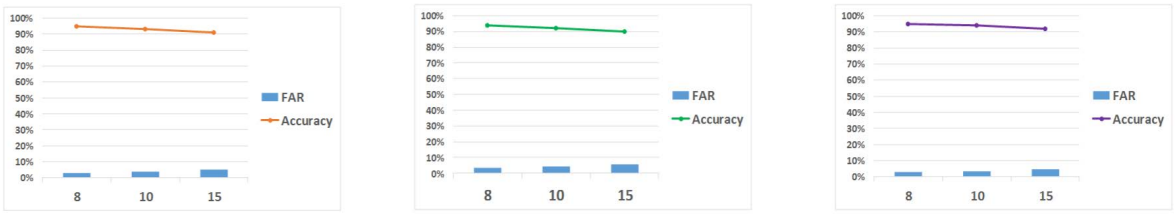
We have tested our biometric-PKI authentication system on FVC2002 DB2-B database [11]. FVC2002 DB2-B contains 80 live-scanned fingerprints, which each fingerprint has eight different impressions. All images are captured in an optical sensor with a resolution 569 dpi. In our experiment, we chose No.1, 2, 7, 8 impression images each finger because other impression images are captured with the intentional displacement. For an authentication system, users are willing to provide good quality fingerprint images. Hence, abnormal images were excluded in our experiment. A fingerprint template was created containing consistent features of two fingerprints and other two fingerprint images were employed for the biometric authentication. For an identical number of matching of each fingerprint, the number of consistent features were limited as 40. We varied quantization factor q_d that $q_d = 8$, $q_d = 10$, and $q_d = 12$. In addition, we varied quantization factor q_θ that, $q_\theta = 8$, $q_\theta = 10$, and $q_\theta = 15$. The size of RSA public key bit stream for the test was 2048-bit. In our experiment, we divided a public key into 128 coefficients. **Table 1** shows the false acceptance rate, the false rejection rate, and the accuracy when $q_d = 8$ with different quantization factors for difference of orientation. **Figure 3** shows that with different quantization factors for distance, our biometric-PKI authentication system remains to achieve over 90 percent accuracy and approximately 3 percent false acceptance rate. Moreover, the proposed system makes cancelable biometric features, therefore, biometric data is irreversible.

7. Conclusion

We have designed and implemented a biometric-PKI authentication system that provides robust authentication against MITM attack that is deficiency under PKI. In addition, the authentication system makes cancelable biometric features that are irreversible. The proposed system has two authentication processes. Firstly, the PKI

Table 1. Biometric-PKI authentication system performance.

q_θ	*FAR*	*FRR*	*Accuracy*
8	0.02	0.25	0.95
10	0.03	0.30	0.94
12	0.02	0.25	0.95



(a) (b) (c)

Figure 3. FAR and Accuracy of the proposed biometric-PKI authentication system; (a) $q_d = 8$; (b) $q_d = 10$; (c) $q_d = 12$.

authentication performs with a digital certificate. Second, the biometric authentication performs. If two authentications succeed, the public key of a digital certificate is trusted one. Finally, the public key could be employed for data encryption. Based on the experimental results, we observe that the proposed biometric-PKI authentication system achieves low false acceptance rate and high accuracy rate.

Acknowledgements

This work was partially supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract (UD060048AD).

References

[1] Adams, C. and Farrell, S. (1999) Internet X.509 Public Key Infrastructure Certificate Management Protocols. RFC 2510 (Proposed Standard). http://www.ietf.org/rfc/rfc2510.txt

[2] Schaad, J. (2005) Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF). RFC 4211 (Proposed Standard). http://www.ietf.org/rfc/rfc4211.txt

[3] Althobaiti, O.S. and Aboalsamh, H.A. (2012) An Enhanced Elliptic curve Cryptography for Biometric. *Proceedings of the 7th International Conference on Computing and Convergence Technology*, Seoul, 3-5 December 2012, 1048-1055.

[4] Scheirer, W., Bishop, B. and Boult, T. (2010) Beyond PKI: The Biocryptographic Key Infrastructure. *Proceedings of the IEEE International Workshop on Information Forensics and Security*, Seattle, 12-15 December 2010, 1-6. http://dx.doi.org/10.1109/WIFS.2010.5711435

[5] Jain, A., Prabhakar, S., Hong, L. and Pankanti, S. (2000) Filterbank-Based Fingerprint Matching. *IEEE Transactions on Image Processing*, **9**, 846-859. http://dx.doi.org/10.1109/83.841531

[6] Jain, A., Hong, L. and Bolle, R. (1997) On-Line Fingerprint Verification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **19**, 302-314. http://dx.doi.org/10.1109/34.587996

[7] Rao, A.R. (1990) A Taxonomy for Texture Description and Identification. Springer, New York. http://dx.doi.org/10.1007/978-1-4613-9777-9

[8] Hong, L., Wan, Y. and Jain, A.K. (1998) Fingerprint Image Enhancement: Algorithm and Performance Evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **20**, 777-789. http://dx.doi.org/10.1109/34.709565

[9] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. (2009) Handbook of Fingerprint Recognition. 2nd Edition, Springer, London. http://dx.doi.org/10.1007/978-1-84882-254-2

[10] Sotirov, A., *et al*. (2008) Creating a Rogue CA Certificate. http://www.tue.nl/hashclash/rogue-ca/

[11] Maio, D., Maltoni, D., Cappelli, R. and Wayman, J.L. (2002) FVC2002: Second Fingerprint Verification Competition. *Proceedings of the 16th International Conference on Pattern Recognition*, **3**, 811-814. http://dx.doi.org/10.1109/ICPR.2002.1048144